How to Develop a Security Controls Oriented Reference Architecture for Cloud, IoT and SDN/NFV Platforms

Theo Dimitrakos

How to Develop a Security Controls Oriented Reference Architecture for Cloud, IoT and SDN/NFV Platforms

Theo Dimitrakos[1,2]

[1] School of Computing, University of Kent, Canterbury, UK
t.dimitrakos@kent.ac.uk,
[2] CSPL, Huawei Technologies Duesseldorf GmbH, Germany
theo.dimitrakos@huawei.com

Abstract. In this paper we present a security architecture style and approach named *Security Controls Oriented Reference (SCORE) Architecture*. The SCORE Architecture extends commonly used security architecture methodologies by placing particular emphasis on how security controls are specified, refined, implemented, traced and assessed throughout the security design and development life-cycle. It encompasses experience of over 30 years in secure systems design and development and it has been applied in practice for developing security capabilities for on top of advanced Cloud, NFV and IoT platforms.

Keywords: Security Controls, Reference Architecture, Security Risk, Systems Design.

1 Introduction

Modernization represents the changes that every organization must face as the generations of technology, skills and expectations are inevitably replaced by the next ones. Telecom Service Providers (TSP), Cloud Service Providers (CSP) and Enterprises alike prepare for the inevitable impact that Cloud Computing, Software Defined Networks (SDN) with Network Function Virtualization (NFV) and the Internet of Things (IoT) have on how to conduct business and compete.

Cloud, SDN/NFV and IoT are delivery models for technology enabled services that drive greater agility, speed and cost savings. Although used in different scope, they all provide on-demand access via a network to an elastic pool of interconnected computing assets (e.g. devices, services, applications, frameworks, platforms, servers, storage, and networks) that can be rapidly provisioned and released with minimal service provider interaction and scaled as needed to enable pay per use. They enable faster delivery of services and on premise cost savings they to optimise the time from idea to solution. They also depend on complex supply networks and ecosystems with shared responsibility models for their delivery and operation. Enterprises will typically consume applications, compute services or devices offered and sometimes also operated by multiple providers. TSP and CSP will often deliver and operate platforms that are developed by many different vendors and whose operations and maintenance

(O&M) often involves one or more third parties. In a platform provider, different product lines focus on but interdependent products and services that are later integrated into a Cloud, NFV or IoT platforms. Reference architectures and shared responsibility models are essential tools to govern and align such complex development, integration and O&M ecosystems.

An architectural style [1], [2] is a named collection of architectural design decisions that can be applied to a specific information system and operation context in order constrain and guide architectural design decisions in that context and elicit beneficial qualities in the resulting system. A reference architecture (RA) provides a method and template solution for developing an architecture for a particular domain. It also provides a common set of concepts which stress commonality. It is an architecture where the structures and respective elements and relations provide templates for concrete architectures in a particular domain or in a family of software systems.

A security reference architecture (SRA) for Cloud, NFV or IoT platforms is a RA that focuses on: *a)* the specification of common security capabilities that are fulfilled by security services and the design of blue-prints for such services; and *b)* the specification of security requirements that need to be fulfilled by the platform and the design of platform enhancements to fulfill these requirements (leveraging where appropriate the security services). It is not the design of a final solution but a baseline that enables aligning platform development and optimizing service delivery and business operation. SRAs for Cloud, NFV and IoT platforms and services are important for a variety of reasons including the following:

- Provide a reference model for security architecture and security policy to those who have a project to produce or use NFV deployments on public or private cloud infrastructures or inter-cloud software-defined overlay network services that enable IoT.
- Enable effective communication of technical solutions, security impact and development strategy to the senior management of a provider and their customers
- Offer guidance for mission-specific product designs that work together.
- Combine knowledge from TSP and CSP with experts from the Cloud, NfV and SDN security communities (e.g. in ETSI, IETF, CSA, ISF).
- Capture relevant security standards and where appropriate align with them.

In this paper we present a security architecture style and approach named Security Controls Oriented Reference (SCORE) Architecture, which extends commonly used security architecture methodologies by placing particular emphasis on how security controls are specified, refined, implemented, traced and assessed throughout the security design and development lifecycle.

The motivation for SCORE Architecture has been to build into the platform design and development processes the ability to: *1)* explain in a structured how security and compliance requirements are satisfied by the system design and implementation; *2)* continuously assess if security and compliance requirements are met to a satisfactory degree; *3)* ensure the mechanisms satisfying these requirements offer a sufficient level of assurance; *4)*ensure clear methods of collecting evidence about the ICT system's conformance to these requirements.

2 Basic concepts

The key concepts used in the SCORE Architecture approach are the summarized in **Fig. 1** and detailed in the subsequent sections. .

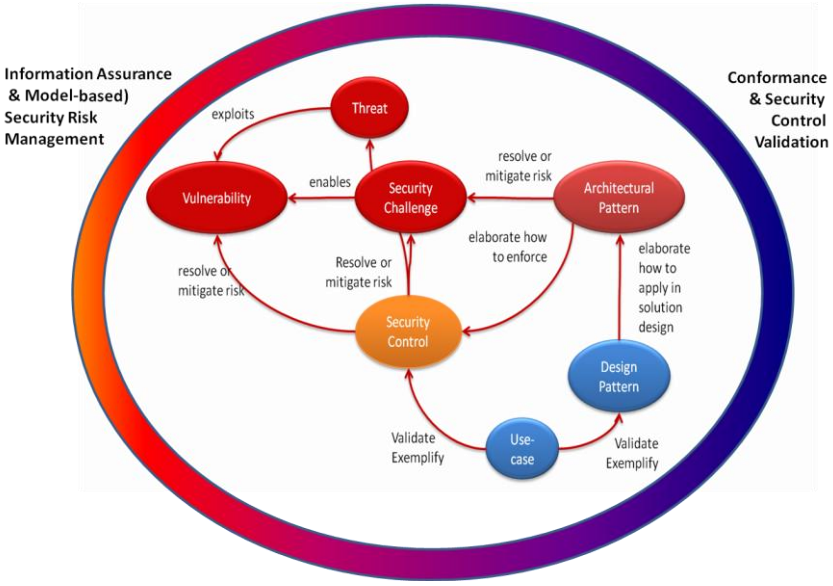

Fig. 1: Overview of the main concepts used in the SCORE Architecture approach.

2.1 Information Assurance, Risk, Continuous Monitoring and Validation

Information Assurance (IA) [3] [4] is about assuring information and managing risks related to the use, processing, storage and transmission of information and data and to the systems and processes used for this purposes. Security risk management [5], [6], [7] provides an overall framework guiding the selection of security controls in relation a security (impact/risk) classification. When combined with continuous monitoring [8], evidence-based validation of security control implementation, regular controls update and risk re-assessment, it enables risk-based decision-making and adaptation for security adaptation, and resilience through tailoring and enhancing of security controls and validating the correctness and effectiveness of their implementation.

2.2 Security Threats and Threat Assessment

We define security threat as any circumstance or event with the potential to adversely impact organizational operations of the carrier or enterprise (including mission, functions, image or reputation), organizational assets, individuals, other organizations, or the nations served by the carrier through the NFV platform via unauthorized access, destruction, disclosure, modification of information, and/or denial of

service. Typically, a threat source realizes a threat by exploiting some vulnerability. A threat may also be enabled by a security challenge either by means of directly enabling some vulnerability or by means of enabling a threat source to exploit another vulnerability of the system that is not directly caused by the security challenge.

Adapting [4], we define Threat Assessment as the formal description and evaluation of threat to the information system that contains the NFV platform.

NIST guidance documents [9] and [10] also offer a similar definition of threat and threat source: a threat is seen as the potential for a threat source to exercise (accidentally trigger or intentionally exploit) a specific vulnerability, where a threat source is either 1) the intent and method targeted at the intentional exploitation of a vulnerability or 2) a situation and method that may accidentally trigger a vulnerability.

2.3 Vulnerability and Vulnerability Assessment

Vulnerability is a weakness in an information system of the NFV platform, system security procedures, internal controls, or implementation that could be exploited or triggered by a threat source. Vulnerability assessment (or vulnerability analysis) [4] is the systematic examination of a (socio-technical) information system containing the NFV platform in order to determine the adequacy of security measures, to identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

2.4 Security Challenges

A "*security challenge*" is a technological, operational, policy or business shortcoming, unresolved technical issue, design, implementation choice or operational complexity that may possibly give rise to vulnerabilities or enable a threat actor to exploit vulnerabilities. Security challenge may often be the security side-effects of a desired and necessary functionality of the system.

One can argue that the effects of security challenges may be split into threats and vulnerabilities and therefore reduce or remove the need for capturing and recording security challenges. However our experience with applying security architecture best practice is that threats and vulnerabilities resulting from security challenges have complex interdependences and characteristic causality which may result in implicit but distinct semantic differences compared to a similar vulnerability caused by external factors. Security challenges for systems conforming to the ETSI NFV Reference Architecture implemented on top of a Cloud (IaaS) NFVI are provided in [13] and [14]. These are consistent with, and more comprehensive than, previous security challenges and requirements elicited by ETSI [15] and CSA [16], [17].

2.5 Security Requirements

A security requirement is a requirement levied on the information system and organization that contains or operates the NFV platform. It is derived from mission or business needs, regulation, legislation, directives, organizational policies, standards, threat

analyses, risk management advisories, guidance and procedures in order to ensure the confidentiality/privacy, integrity, accountability and availability of information (including data and software) that is being processed, stored or transmitted.

2.6 Security Controls and Security Control Assessment

Security controls are the safeguards/countermeasures prescribed for information systems or organizations that are designed to: protect the confidentiality/privacy, integrity, accountability and availability of information that is processed, stored and transmitted by those systems/organizations; and to satisfy a set of defined security requirements [11]. A security control resolves or mitigates the risk associated with some threat either by correcting an existing vulnerability or by preventing a security challenge enable vulnerabilities or by preventing vulnerability exploitation by a threat source. A security control must come together with metrics for assessing the level of assurance of its implementation.

A *Security Control Baseline* [5] is the set of minimum security controls that provides a starting point for the *"security controls tailoring"* process [11]: *(i)* identifying and designating common controls; *(ii)* applying scoping considerations on the applicability and implementation of baseline controls; *(iii)* selecting compensating security controls; *(iv)* assigning specific values to organization-defined security control parameters; *(v)* supplementing baselines with additional security controls or control enhancements; and *(vi)* providing additional specification information for control implementation. Security controls may also be enhanced as part of tailoring in order to: *a)* build in additional, but related, functionality to the control; *b)* increase the strength of the control; or *c)* add assurance to the control.

Security Control Inheritance [4] means that an information system receives protection from security controls (or portions of security controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides.

Security Control Assessment is the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended and producing the desired outcome with respect to meeting the security requirements for an information system or organization [4].

2.7 Architectural and Design Patterns

An architectural pattern is a rigorous description in a specific architectural style that solves and delineates some essential cohesive elements of a system architecture. The functionality described by an architectural pattern is sometimes referred to in the literature as a Common Capability [18].

A design pattern elaborates how to apply the architectural pattern into a specific information system or product implementation and how to collect the corresponding evidence to asses both conformance to the architectural pattern and the fulfillment of

the corresponding security controls. Different system or solution architectures may implement the same patterns [19].

Architectural and design patterns should be used to elaborate how security controls are realized and enforced and what is the required evidence to fulfill the level of assurance of the control implementation. It should then also capture dependences between security controls, trace their relationship to security challenges and security requirements and evidence how a collection of security controls resolve or mitigate corresponding threats and vulnerabilities. Use-cases should be used as the preferred means of explaining by means of exemplar scenarios how threats and vulnerabilities are resolved or mitigated via the application of security controls as realized by the corresponding architectural patterns.

3 SCORE Architecture Process

A simplified overview of the architecture development process used in the SCORE Architecture approach is described in Fig. **2**: In this section we elaborate each stage of this process.

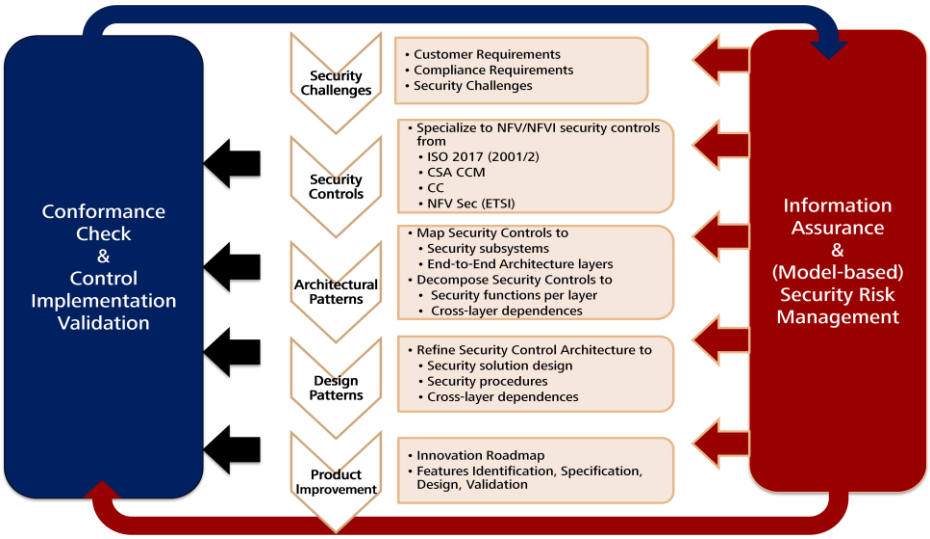

Fig. 2: Simplified overview of the process that underpins the SCORE Architecture

3.1 Information Assurance: a Security Risk Management

Risk Management and *Information Assurance* are continuous governance processes that govern the assessment and impact analysis of threats, vulnerabilities and security challenges and the selection, adaptation and refinement ("tailoring") of security controls as well as risk associated with the sufficiency of the selected security control implementations. Security risk management and information assurance are enacted

during and in between these sequentially linked steps and they may trigger iteration from any sequentially linked design and development stage to any preceding stage. The SCORE Architecture recommends that NCSS/NIST Risk Management Framework (RMF) [20] enhanced with the guidance of ENISA publications "Cloud Computing Risk Assessment" [21] and "Cloud Computing Information Assurance" [22]. The following **Fig. 3** summarizes the risk management steps.

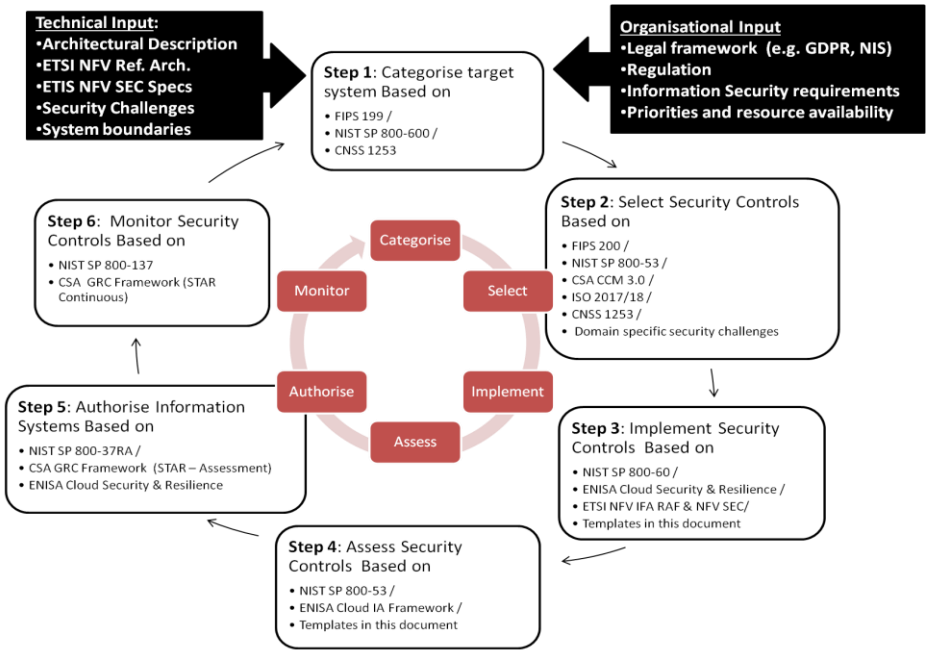

Fig. 3: Extending NIST RMF in accordance to the SCORE Architecture framework

3.2 Architectural Conformance and Implementation Validation

Typically the implementation of security controls is validated by internal and third party security auditors and certification authorities. However, in order to improve security and privacy by design through continuous improvement and alignment between control definition and implementation, SCORE Architecture recommends that *architectural conformance and implementation validation* is enacted as a continuous process complementing risk management and information assurance. First the conformance of the design and implementation of a control to the specification of the control is ensured, then once implementation is approved the conformance of the implementation with the design and architecture patterns is assured in addition to the validation of the implementation. The SCORE Architecture requires that every control comes together with:

- Conformance guidance: qualitative information and metrics on how to assess conformance of the control architecture. Each architectural pattern contains criteria that must be met by the conformant design patterns.
- Validation metrics and requirements: test-cases, metrics, validation criteria and qualitative guidance that help validate the correctness of the implementation of a control. This may be similar to what certification bodies and auditors would require when assessing the system.
- Evidence collection requirements: a classification of the data that need to be collected for substantiating conformance and validation together with guidance on the preferred evidence collection methods.

Additional techniques that can help with achieving design conformance are mentioned in [22] and some of them have been applied to a case study on CryptoDB [23].

3.3 Architecture Design Process

In this section we describe the design and development process of SCORE Architecture. Although the design and development steps are presented in a sequence, the SCORE Architecture prescribes iterations of varying scope and frequency which are determined by the information assurance and risk management process in conjunction with the results of the architectural conformance and validation process.

Threats and Challenges

The starting point of the SCORE Architecture design process is the *Security Challenges Analysis Phase*. Analysis of threats and vulnerabilities on the basis of the organizational (e.g. carrier operations) and information system requirements (e.g. VNFs, NFV platform, cloud platform, datacenters), any anticipated compliance requirements and of the security challenges (e.g. [11]) associated with the targeted platform architecture. This should be complemented by a (model-based) Security Risk Assessment based on [9] which may be enhanced with other security risk analysis methods such as OCTAVE [24] or COBRA for assessing security risk related to human centric processes or FRAP [25] and m CORAS [26] and [27] for assessing information system or product / platform risks. Risk and impact should be classified so as to enable a base line of control for each risk acceptance and impact level and also be traced by to the associated threats, vulnerabilities and organizational or compliance requirements.

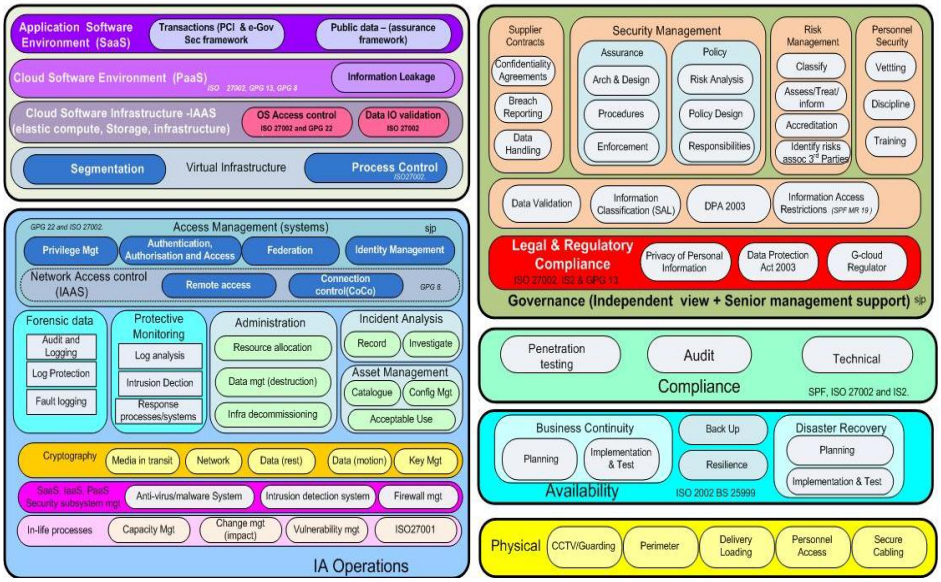

Fig. 4: Indicative categorization for a catalog (repository) of relevant security controls

Security Controls

An important stage of the SCORE Architecture process is the elicitation and specification of the specific security controls for the system being architected. The security controls underpin the risk management process and provide a reference for the information assurance process. They also scope and steer the development of security architectural patterns and consequently design patterns and their imprint must be traceable and measurable (or assessable) in every step from information system design to the targeted application and platform implementations. The elicitation and specification of security controls typically includes the following steps: *1)* Security control catalog selection; *2)* Security categorization; *3)* Security control base-line determination; *4)* Security control tailoring.

Security control repository and catalog selection: Defining the security controls catalog form a repository of security controls. For Cloud, IoT and NFV platforms, SCORE Architecture recommends a base-line for the security controls repository (**Fig. 4**) based on ISO/IEC 27017 extending ISO/IEC 27001 and 27002 complemented with CSA Cloud Controls Matrix including their reference to the scope of applicability of each control. **Fig. 4**: summarizes an indicative collection and classification of relevant security controls based on CSAISO/IEC 27001 and 27017/27018

Security categorization: Determining the criticality and sensitivity of the information to be processed, stored, or transmitted by the target platform including the corresponding Operation and Maintenance (O&M) processes. *FIPS Publication 199* [28] offers commonly referenced security categorization. SCORE Architecture the follow-

ing formula in for describing impact, where the acceptable values for potential impact are *low*, *moderate*, or *high*. This formula extends [28] with additional security objectives relating to privacy and accountability in order to accommodate recent regulations in Europe relating to the implementation of GDPR [28] and NIS directive [29]:

Security_Category = {(confidentiality, impact), (privacy, impact), (integrity, impact), (accountability, impact), (availability, impact)}.

Following the security categorization, security controls are then selected as countermeasures to the potential adverse impact described in the results of the security classification. **Fig. 5** summarizes the security control selection and tailoring process described in this section and the corresponding documentation extending [16] and [31].

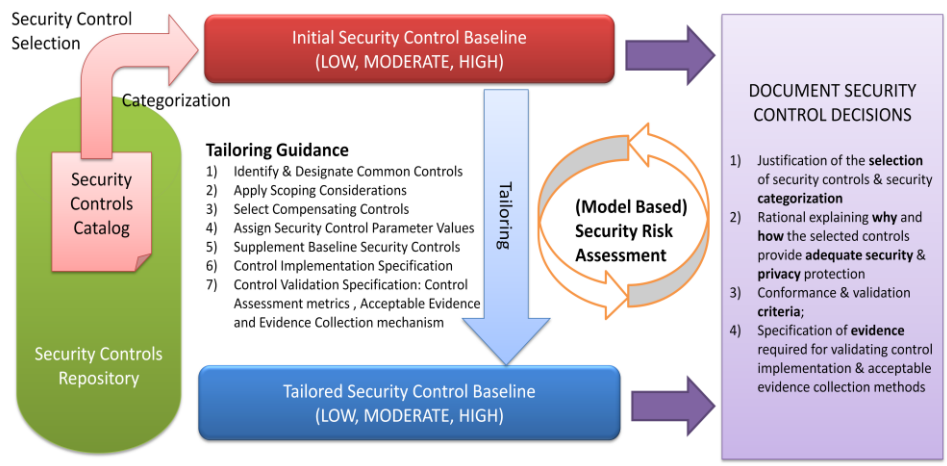

Fig. 5: Summary of the security controls selection and documentation

Security controls baseline definition: determining the most cost-effective, appropriate set of security controls, which if implemented and determined to be effective, would mitigate security risk while complying with security requirements and security challenges defined in the previous phase. To assist organizations in making the appropriate selection of security controls, NIST defines the concept of *baseline controls* [11]. Baseline controls are the starting point for the security control selection process. Furthermore [11] in Appendix D defines three security control base-lines in accordance with FIPS Publication 199 and FIPS Publication 200.

The security controls must be carefully reviewed and revised periodically to reflect experience gained from using the controls, directives and regulations, changing security requirements and new or emerging threats, vulnerabilities, and attack methods as well as new security challenges resulting from the emergence of new technologies. Also security controls catalogs may be specialized for different regions to reflect differences in legislation.

Once the applicable security controls baseline has been selected, the controls in the baseline need to be tailored.

Security controls tailoring: to modify appropriately and align the controls more closely with the specific conditions of the targeted system and its intended context of operation. Security controls must not be removed at any stage from the baseline to serve operation convenience. The following tailoring activities must be approved by authorizing officials in coordination with selected organizational officials:

- Identifying and designating common controls in initial security control baselines;
- Applying scoping considerations to the remaining baseline security controls;
- Selecting compensating security controls, if needed;
- Assigning specific values to organization-defined security control parameters via explicit assignment and selection statements;
- Supplementing baselines with additional security controls and control enhancements, if needed – see [11] and [31] for details and references to examples of recommended supplementary security controls;
- Providing additional specification information for control implementation, if needed.

Every security control from a baseline must be accounted for either by the organizations consuming or operating the service or by the product or platform owner. Each of these actors must determine which controls are implemented solely by the actor, which correspond to shared responsibility and which are implemented by another of these actors.

Documenting security controls: it is necessary to document all relevant decisions take during the security control selection process. Such documentation provides a very important input in assessing the security of a system in relation to the potential mission or business impact. This documentation together with supporting evidence about the correctness and conformance of the security control implementations provides valuable information for information assurance, architectural improvements, change or revision and compliance assessment or accreditation. It also constitutes a reference document for NFV platform providers, VNF developers, Cloud IaaS providers, carriers and enterprises understanding how to implement shared or common controls and control overlays.

Architectural and Design Patterns Definition

This phase of SCORE Architecture starts by mapping security controls to the different layers and components of the target system. In this mapping, security controls provide the common technical requirements for the elicitation of common capabilities which are documented by means of architectural patterns. Detailed examples of how to elicit common technical requirements and identify common capabilities for cloud platforms are provided in [18]. An illustrative high level overview of such a mapping is provided in **Fig. 6**.

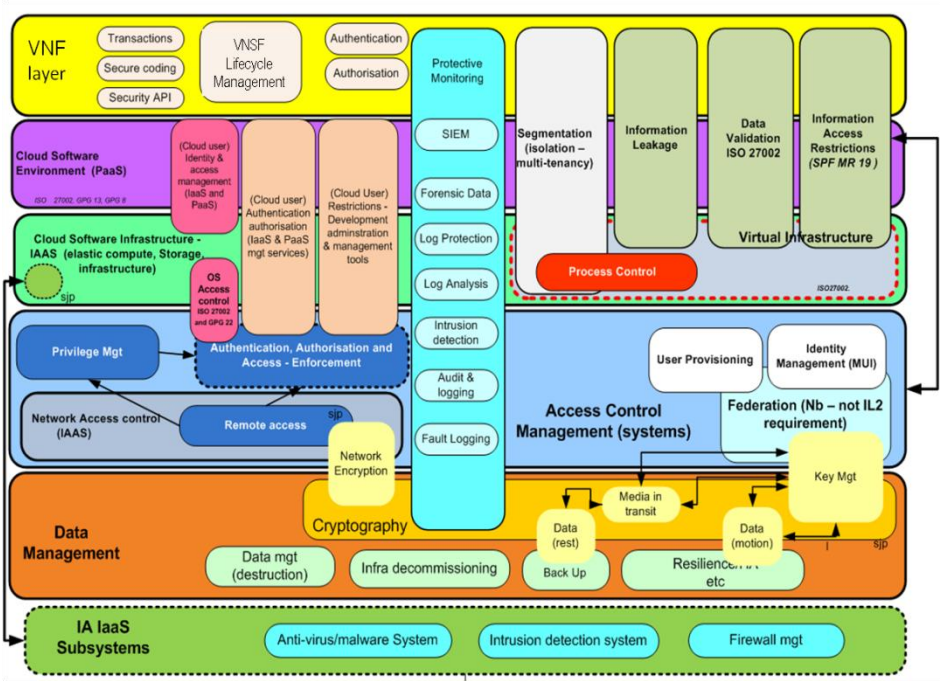

Fig. 6: Mapping security controls into subsystems of the NFV/Cloud platform layers

In addition to defining common (security) capabilities and their architectural or design patterns, conformance and traceability must be assured and maintained. SCORE Architecture provides templates for architectural and design patterns that ensure:

1) Specifying which security controls are satisfied by the pattern;
2) Explain how the requirements, description, intend and dependences are met by the pattern for each referenced security control;
3) Specifying criteria, metrics and preferred conformance validation methods for ensuring conformance of subsequent design patterns to the architectural pattern;
4) Specifying criteria, metrics and preferred methods for validating the implementation of the architectural or design pattern and for collecting evidence that is suitable to support such validation.

The dependences to other design patterns – including those describing relevant information models as well the application of relevant policies and procedures – must be specified explicitly. Typically design pattern dependences inherit and extend architectural pattern dependences. The implementation results in interdependent subsystem. It is therefore very important to ensure traceability of dependences and validate it as part of architectural conformance. Furthermore, technical use-cases (decomposing and refining the generic use-cases used for common capabilities and architectural patterns) should be used in order to describe the functionalities and usage scenarios of the corresponding design patterns. It is recommended that refinement of archi-

tectural pattern to design pattern is aligned with and informed by the refinement of general use-case through to technical use-cases and its decomposition to several sub-use cases.

Product Improvement
The SCORE Architecture also includes guidelines for product improvement that are consistent with system engineering methods such as IPD, ISC and Agile. These guidelines comprise:

- Guidance on (product) features identification, specification, design, validation including (1) design specialization; (2) prioritization of technical requirements and templates to assist this prioritization ; (3) GAP analysis against the prioritized requirements and templates to assist this analysis ; (4) Change impact assessment and (5) change management; (6) Time-line definition
- Guidance on defining an innovation roadmap and a product improvement time-line in order to guide future enhancements and identified shortcomings. SCORE provides templates to assist innovation roadmap creation and maintenance.

4 Conclusion

In this paper I presented a method for developing reference security architectures for distributed information systems such Cloud, IoT and NFV platforms. This approach reflects over 20 years of research and incorporates methodologies developed through analysis and experimentation in [17] (where 100 organizations conducted 25 experiments in Enterprise use of Cloud Computing) with model-based risk analysis (e.g. [26] and [27]) and guidance from NIST, ENISA, ETSI, ISO and CSA. In its current form, the SCORE Architecture approach has been used for developing reference architectures of innovative security capabilities for intrusion prevention and data protection in multi-provider clouds in the context of EIT Digital High Impact Initiative on Trusted Cloud in cooperation where BT, TIM and Huawei participated. It has also been validated in additional use-cases with KDDI Research and it is currently being used by security researchers in Huawei for developing security reference architectures for NFV and Hybrid Cloud platforms.

References

1. R. N. Taylor, N. N. Medvidović and E. M. Dashofy, Software architecture: Foundations, Theory and Practice, Wiley,, 2009.

2. M. Shaw and D. Garlan, Software architecture: perspectives on an emerging discipline, Prentice Hall, 1996.

3. R. Kissel, "Glossary of Key Information Security Terms (NISTIR 7298 Revision 2),"

NIST (National Institute of Standards and Technology), 2013.

4. CNSS, "National Informaiton Assurance (IA) Glossary. CNSS Instruction No. 4009," National Security Agency (NSA), 2003.

5. FIPS, "Minimum Security Requirements for Federal Information and Information Systems (FIPS 200)," FEDERAL INFORMATION PROCESSING STANDARDS, 2006.

6. NIST, "Guide for Applying the Risk Management Framework (RMF) to Federal Information Systems: a Security Life Cycle Approach," National Institute of Standards and Technology, 2010 (Updated 2014).

7. NIST, "Risk Management Framework forInformation Systems and Organizations: A System Life Cycle Approach for Security and Privacy (DISCUSSION DRAFT)," 2017.

8. K. Dempsey, N.S. Chawla, A. Johnson, R. Johnston, A.C. Jones, A. Orebaugh, M. Scholl, K. Stine, "Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations," National Institute of Standards and Technology, 2011.

9. Joint Task Force Transformation Initiative, "Guide for Conducting Risk Assessments (NIST SP 800-30r1)," National Institute of Standards and Technology, 2012.

10. G. Stoneburner, A. Goguen and A. Feringa, "Risk Management Guide for Information Technology Systems," NIST - National Institute of Standards and Technology, 2002.

11. JOINT TASK FORCE, "Security and Privacy Controls for Federal Information Systems and Organizations," National Institute of Standards and Technology, 2013.

12. ETSI, "Network Functions Virtualisation (NFV); Architectural Framework," The European Telecommunications Standards Institute , 2013.

13. T. Dimitrakos, "Security Challenges and Guidance for Protecting NFV on Cloud IaaS," ETSI NFV Security Week, 2017. [Online] https://docbox.etsi.org/workshop/2017/201706_SECURITYWEEK/05_NFVSECURITY

14. T. Dimitrakos, "Towards a security reference architecture for Network Function Virtualisation: security challenges and security controls," NECS, 2017.

15, ETSI, "Network Functions Virtualisation (NFV);. NFV Security;. Security and Trust Guidance.," The European Telecommunications Standards Institute, 2014.

16, CSA, "Network Function Virtualization," CSA, 2016.

17, CSA, "Best Practices for Mitigating Risks in Virtualized Environments," CSA, 2015.

18. T. Dimitrakos, Service Oriented Infrastructures and Cloud Service Platforms for the Enterprise. A selection of common capabilities validated in real-life business trials, J. M.

S. W. Theo Dimitrakos, Ed., Springer, 2009.

19. R. N. Taylor, N. Medvidovic and E. M. Dashofy., Software Architecture: Foundations, Theory, and Practice., Wiley Publishing, 2009.

20. NIST, "Risk Management Framework (RMF) Overview," 30 November 2016. [Online].

21. ENISA, "Cloud Computing Benefits, risks and recommendations for information security," European Network and Information Security Agency, 2009.

22. ENISA, "Cloud Computing: Information Assurance Framework," The European Network and Information Security Agency, 2009.

23. M. Abi-Antoun and J. M. Barnes, "Analyzing security architectures," in *IEEE/ACM international conference on Automated software engineering (ASE'10)*, 2010.

24. R. A. Caralli, J. F. Stevens, L. R. Young and W. R. Wilson, "Introducing OCTAVE Allegro: Improving the Information Security Risk Assessment Process," Publisher: Software Engineering Institute CMU/SEI Report Number: CMU/SEI-2007-TR-012, 2007.

25. T. R. Peltier, Information Security Risk Analysis, Third Edition, CRC press, 2010.

26. R. Fredriksen, M. Kristiansen, B. A. Gran, K. Stølen, T. A. Opperud and T. Dimitrakos, "The CORAS Framework for a Model-Based Risk Management Process," *International Conference on Computer Safety, Reliability, and Security (SAFECOMP)*, 2002.

27. M. S. Lund, B. Solhaug and K. Stolen, Model-driven risk analysis - The CORAS Approach, Springer, 2011.

28. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, REGULATION (EU) 2016/679 *Official Journal of the European Union*, 2016.

29. THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION, "DIRECTIVE (EU) 2016/1148. *Official Journal of the European Union*, 2016.

30. K. Stine, R. Kissel, W. C. Barker, J. Fahlsing and J. Gulick, "Volume I: Guide for Mapping Types of Information and Information Systems to Security Categories," National Institute of Standards and Technology, 2008.

31. Cloud Security Alliance (CSA), "Cloud Controls Matrix," 9 January 2017. [Online]. Available: https://cloudsecurityalliance.org/group/cloud-controls-matrix/..

32. Software Engineering Institute, "Architecture Conformance," [Online]. Available: https://www.sei.cmu.edu/architecture/research/previousresearch/conformance.cfm.